UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

UNITED STATES OF AMERICA	)	
	)	
v.	)	1:12-cr-
	)	
ANIL KHEDA	)	

INDICTMENT

The Grand Jury charges:

Introduction

At all times material to this Indictment

1. ANIL KHEDA, also known by online monikers that include "Master," "Master Anil," "Riotist," and "SnoopDoggOW," resided in the Netherlands. He is the operator of an online game called "Outcraft," which he launched in or about January 2008.

2. UNINDICTED CO-CONSPIRATOR ONE ("UC ONE"), also known by online monikers that include "xPimpster1337," and "Pimpster," is a juvenile with the initials W.G., who resided in the United Kingdom.

3. KHEDA and UC ONE are avid players of internet-based, multi-player interactive computer games, including a game called "Outwar."

4. Rampid Interactive LLC ("Rampid") is a company based in Portsmouth, New Hampshire, that creates, publishes, and hosts internet-based, multi-player interactive computer games, including "Outwar." Rampid created and published "Outwar" in or before 2002-03.

5. "Outwar" has over 75, 000 active players worldwide. It is what is known in the gaming industry as a "massive, multi-player online role-playing game" ("MMORPG"). Typically, in an MMORPG like "Outwar," a large number of players interact

simultaneously online with one another in a fantasy-based virtual world where each player assumes a fictional role and competes with other players.

6. MMORPGs like “Outwar” often feature a character progression element, where a player’s fictional character evolves and develops over time as the player continues to play the game. Progression may be measured with points, levels, titles, and the like. A player earns these metrics by successfully completing a task, winning a battle, and the like. These metrics remain with the player over time, from one online session to another, even when the player is not actively playing.

7. Players create a character in the “Outwar” game, and they can begin playing the game free of charge. As a player continues to play "Outwar" over time, the player gains points or other items that improve the player’s standing or status. Optionally, "Outwar" players can also purchase points from Rampid in order for their character to more rapidly progress.

8. “Outwar” players connect over the internet to Rampid’s gaming environment/“world,” which Rampid continuously runs on its multiple computer servers.

9. As an integral part of operating “Outwar,” Rampid maintains a “users’ table” on its computer servers. The “users’ table” (also referred to as its “users’ database”) is a database containing all of the “Outwar” players’ game information, including their previously acquired points and other measurements of their characters’ progression. With no “users’ table,” there are no players in the game and the game is therefore not playable.

10. As an integral part of “Outwar,” Rampid has designed and maintained the proprietary and confidential “source code” for “Outwar” which is the software program responsible for the game play and game design.

11. From in or about November 2007 to in or about August 2008, KHEDA, UNINDICTED CO-CONSPIRATOR ONE, and other members of the conspiracy (1) accessed Rampid's computer servers, without authorization, and disabled "Outwar," rendering it unplayable for days at a time; (2) accessed Rampid's computer servers, without authorization, and altered user accounts that caused the restoration of suspended Outwar player accounts and the accrual of unearned additional "points"; (3) accessed Rampid's computer servers, without authorization, and obtained a copy of all or portions of the "Outwar" computer source code, which they then used to help create a competitor online game, "Outcraft"; and (4) sent Rampid interstate communications threatening to continue hacking into Rampid's computer systems unless Rampid agreed to pay them money or provide them with other benefits.

12. Ultimately, as a result of the defendants' hacking activities, Rampid was unable to operate "Outwar" for a total of almost two weeks over a nine-month period and incurred over one hundred thousand dollars in lost revenues, lost wages, lost hosting costs, long term loss of business, as well as the loss of exclusive use of their proprietary source code, which it had invested approximately $1.5 million in creating. KHEDA earned approximately $10,000 in profits from operating a competitor game, "Outcraft," derived from fees he charged players. "Outcraft" has approximately 10,000 players worldwide.

COUNT ONE
Conspiracy to Commit Computer-Related Fraud
(18 U.S.C. §§ 371 and 1030(a)(2), (4), (5) & (7))

13. The allegations set forth in paragraphs 1 through 12 are re-alleged and incorporated as if set forth herein in their entirety.

14. Beginning at a date uncertain, but at least as early as November 2007, and continuing to a date uncertain, but at least as late as August 2008, in the District of New Hampshire and elsewhere, the defendant,

ANIL KHEDA

knowingly and intentionally combined, conspired, and agreed with UNINDICTED CO-CONSPIRATOR ONE and with other persons known and unknown to the Grand Jury, to commit offenses against the United States, namely,

(a) intentionally accessing a protected computer without authorization and exceeding authorization, and thereby obtaining information (including the Outwar users' table, player database, and game source code), and the offense was committed for purposes of commercial advantage and private financial gain, and was committed in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States or of any state; and the value of the information obtained exceeded $5,000, all in violation of 18 U.S.C. §§1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii);

(b) knowingly, and with intent to defraud, accessing a protected computer without authorization, and exceeding authorized access, and by means of such conduct furthering the intended fraud and obtaining anything of value (including the Outwar users' table,

player database, game source code, $1,500, restoration of suspended Outwar player accounts, unearned additional "points"), in violation of 18 U.S.C. §1030(a)(4);

(c) knowingly causing the transmission of a program, information, code, and command, and as a result of such conduct, intentionally causing damage without authorization (including deletion of the Outwar users' table, player database, and copying of source code; alteration of user accounts that caused the restoration of suspended Outwar player accounts, and unearned additional "points"), to a protected computer, in violation of 18 U.S.C. §1030(a)(5)(A); and

(d) with intent to extort from any person any money and thing of value, transmitting in interstate and foreign commerce any communication containing any (A) threat to cause damage to a protected computer, (B) threat to obtain information from a protected computer without authorization and in excess of authorization, and (C) demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate extortion, in violation of 18 U.S.C. §1030(a)(7)(A)-(C).

Objects of the Conspiracy

15. It was the object of the conspiracy for defendants KHEDA, UC ONE, and others to access Rampid's computer network without authorization to (1) disable "Outwar," rendering the game unplayable and in turn use this as leverage to attempt to extort money and other benefits from Rampid, (2) alter user accounts in "Outwar" to obtain benefits for defendants, including unsuspended account status and additional points, and (3) obtain a copy of all or portions of "Outwar's" confidential and proprietary game source code and in

turn use this to create a competitor game, "Outcraft."

15. It was also the object of the conspiracy for defendants KHEDA, UC ONE, and others to send Rampid interstate communications threatening to continue hacking into Rampid's computer systems, unless Rampid agreed to pay them money or provide them with other benefits.

Manner and Means of the Conspiracy

16. It was part of the conspiracy that defendants KHEDA, UC ONE, and others, acting without authorization, remotely accessed various portions of Rampid's computer network.

17. It was further part of the conspiracy that defendants KHEDA, UC ONE, and others, then copied and obtained information from Rampid's computer network, including the Outwar users' table, database, and portions of its source code.

18. It was further part of the conspiracy that defendants KHEDA, UC ONE, and others used portions of the information they obtained from Rampid's computer network, including portions of the "Outwar" source code, in order to create and operate a competitor game, "Outcraft."

19. It was further part of the conspiracy that defendants KHEDA, UC ONE, and others, then deleted information from Rampid's computer network, including the Outwar users' table, which in turn rendered the game unplayable for days at a time.

20. It was further part of the conspiracy that defendants KHEDA, UC ONE, and others, then modified various files on Rampid's computer network, which in turn unsuspended the defendants' previously suspended accounts and provided them with other benefits.

21. It was further part of the conspiracy that defendants KHEDA, UC ONE, and others, then attempted to use their computer intrusions as leverage to try to extort money and other benefits from Rampid.

22. It was further part of the conspiracy that defendants KHEDA, UC ONE, and others, then engaged in e-mail and chat and telephone communications with various Rampid employees, where they threatened to continue their hacking unless they received money or other benefits. Alternatively, they offered to refrain from further hacking and reveal their hacking techniques, in exchange for money or other benefits.

Overt Acts

23. In furtherance of the conspiracy, and to effect and accomplish the objects of it, one or more of the defendants or conspirators, both indicted and unindicted, committed, among others, the following over acts in the District of New Hampshire and elsewhere:

24. On or about November 29, 2007, members of the conspiracy accessed Rampid's computer networks without authorization and made modifications to various Outwar players' user accounts, which in turn prompted Rampid to delete the player accounts of "Master" and "xPimpster1337."

25. On or about November 30, 2007, members of the conspiracy accessed Rampid's computer networks without authorization and deleted the "Outwar" users' table, which in turn made "Outwar" unplayable for several days.

26. On or about November 30, 2007, KHEDA, using the online moniker "SnoopDoggOW" engaged in a chat communication with a Rampid employee named "Nick," where KHEDA threatened to retaliate for having his "Master" account suspended.

SnoopDoggOW (2:40:19 PM):no, you will pay for deleting master
SnoopDoggOW (2:40:21 PM):maybe not now
SnoopDoggOW (2:40:24 PM):but in some months
SnoopDoggOW (2:40:25 PM):or years
[Employee at Rampid] (2:38:37 PM):wow alright

27. On or about November 30, 2007, KHEDA, using the online moniker "SnoopDoggOW" engaged in a chat communication with a Rampid employee named "Justin," where KHEDA acknowledged that his co-conspirators and he deleted the Outwar database (referred to as "db" in the chat below) in retaliation for having their accounts deleted. KHEDA stated that if Rampid let him continuing playing Outwar (referred to as playing a "raid" in the chat below), KHEDA will refrain from further hacking.

(9:04:51 AM) snoopdoggow: we got db [database] just this morning when i saw you deleted us
(9:04:57 AM) snoopdoggow: was playing fair before
(9:05:11 AM) snoopdoggow: but yeah
(9:05:12 AM) snoopdoggow: fuck you
//
//
//
(9:37:55 AM) snoopdoggow: after you deleted us last night we were forced to search and destroy again this morning
//
//
//
(9:44:46 AM) snoopdoggow: bring it up let me do another raid and wont touch anything for a few days
(9:45:02 AM) [Employee at Rampid]: I need everything, I can't leave the game vulnerable
//
//
//
(9:45:31 AM) [Employee at Rampid]: No one will play if they know you have db [database]
(9:45:40 AM) [Employee at Rampid]: and you guys made it pretty obvious.
(9:45:48 AM) snoopdoggow: sucks for you
(9:45:54 AM) [Employee at Rampid]: Guess so

28. In or about November 2007, members of the conspiracy accessed Rampid's computer networks without authorization and obtained a copy of all or a portion of Rampid's source code for "Outwar."

29. KHEDA later used a portion of the Outwar source code to create a competitor game called "Outcraft," which he then launched in January 2008.

30. On or about December 1, 2007, KHEDA, using the online moniker "Master," sent the following e-mail to several Rampid employees:

Hi guys,

I'm sure you all know what happened
Pimpster may have pussed out after [employee at Rampid] called his mom, I'll never talk to that noob snitch again.
However I am still around, you guys probably thought that pimpster has been doing this all by himself, think again noobs. There are lots of things that I kept for myself.
With all the information I have, I can easily re-obtain access on the site again, and this time I will keep it for myself.
You cannot scare me by calling my mom on the phone like you did with pimpster lol, I actually proposed [Rampid employee] to call me so I can tell him how much he sucks, he didn't reply.

You guys have the following 3 options:
1. Let me play again on my master account (with everything that was on it), and I will report everything when I come across a vulnerability
2. Pay me $1500 and you will never hear from me again
3. Don't reply to this email and you are gonna wish you picked one of the other options

Please note, this is not a treatment, it is a promise.

~ Master.

31. Between on or about December 3, 2007, and on or about December 5, 2007, KHEDA, using the moniker "SnoopDoggOW," took part in a number of online chat communications with one or more Rampid employees, acknowledged that his co-conspirators and he deleted several of the Outwar databases (referred to as "db" in the chat below), described

the various computer files that they have copied and deleted from the databases, and asked Rampid to pay him an unspecified amount of money. For example:

December 3, 2007

Rampid [employee] (5:45:35 PM):you want money huh
Rampid [employee] (5:45:41 PM):that's all you want?
SnoopDoggOW (5:46:05 PM): yes
SnoopDoggOW (5:46:17 PM):i dont mind some nasty pictures of stacey
Rampid[employee] (5:51:50 PM):what exactly would I be paying for?
SnoopDoggOW (5:52:01 PM):what are you looking for
Rampid[employee] (5:52:41 PM):answers about if you did anything to our backups, a version of our db's before you deleted them, and any vulnerabilities that you have, Anil
SnoopDoggOW (6:01:38 PM): im sure you can find that out yourself
SnoopDoggOW (6:01:43 PM):i have rg_accounts from rg db
SnoopDoggOW (6:01:46 PM):and from the 5 other dbs; users, crews, items_unique
SnoopDoggOW (6:02:12 PM):and items_data, world_mobs

December 4, 2007

SnoopDoggOW (10:55:35 AM):so its true, only i have recent backups
SnoopDoggOW (10:55:44 AM):since you rolled back to 3 months ago
Rampid[Employee] (10:57:23 AM):nevermind, you've probably tainted them by now
SnoopDoggOW (10:59:01 AM): actually i didnt
SnoopDoggOW (10:59:10 AM):but i doubt would pay me anyway

32. On or about December 24, 2007, KHEDA registered the domain name, "www.Outcraft.com," where he hosted the "Outcraft" game in Amsterdam-Noord, the Netherlands. He was the website owner, tech-contact, and billing contact for the website.

33. Between on or about June 7, 2008, and on or about June 9, 2008, KHEDA, using the moniker "Riotist," participated in a number of online chat communications with employees of Rampid. He threatened to exploit a vulnerability in the software. In exchange for providing details about the vulnerability, he demanded contact information for his co-conspirator. For example:

June 7, 2008

Riotist (7:31:21 PM): im sure you are interested in this point glitch
Riotist (7:31:22 PM): o.O
Riotist (7:31:35 PM): if you dont reply in 12 hours with pimpsters number
Riotist (7:31:42 PM): i will spread these points

June 8, 2008

Riotist (10:13:02 AM): nubert
Riotist (10:13:05 AM): your time is up

34. On or about July 15, 2008, and July 16, 2008, KHEDA, using the online moniker "Riotist," participated in online chat communications with the general manager of Rampid. During these chats, he claimed that he had found a vulnerability in Rampid's computer network that would allow him to access the Outwar database. He offered to disclose the vulnerability to Rampid in exchange for Rampid's restoring his Outwar account. For example:

July 15, 2008

Biz [Rampid employee] (1:35:00 PM):why do you still think we took your money?
Biz [Rampid employee] (1:35:12 PM):you deleted our db multiple times haha
Riotist (1:35:55 PM): yes after you told me i wouldnt get my account or money back
//
//
//
Riotist (1:46:39 PM): i just want to know this ; would you restore my zimbob account if i give you something close to db access
Riotist (1:46:58 PM): what i have atm, can harm you more than ive already done in the past
Riotist (1:47:00 PM): o.O
Riotist (1:47:25 PM): not giving hints but it is worth the deal
Biz [Rampid employee] (1:47:34 PM):I'd have to discuss it with some people... what if we already know about this?
Riotist (1:47:55 PM): then you would have fixed it by now
Riotist (1:48:00 PM): because it is big
Biz [Rampid employee] (1:48:34 PM):what's "close to db access"
Riotist (1:48:42 PM): Riotist (19:47:27): not giving hints but it is worth the deal

35. On or about July 28, 2008, members of the conspiracy accessed Rampid's computer

network without authorization and deleted the Outwar users' table or database, which in turn made Outwar unplayable for several days.

36. On or about July 30, 2008, KHEDA, using the online moniker "Riotist," participated in an online chat communication with Rampid's General Manager. He discussed vulnerabilities in Rampid's computer network that he knew how to exploit. He suggested that he had the ability to gain administrator access in the game. He told Rampid that he wanted to have his user account restored. For example:

July 30, 2008

Riotist (2:00:04 PM): what do i get if i make myself admin 1
[Rampid employee] (2:00:11 PM): a high five!
Riotist (2:00:24 PM): i want my zimbob guy

37. On or about August 1, 2008, members of the conspiracy accessed Rampid's computer networks without authorization and manipulated the user database, posted derogatory comments about the administrators on the website, and posted flattering comments about "Master."

38. In early August 2008, KHEDA, using the online moniker "Riotist," engaged in an online chat communication with the owner of Rampid and made a deal that would allow "Master" to play "Outwar" again. In exchange, KHEDA agreed to provide details of the vulnerability that he claimed to have used to access the administrators' accounts and provide details of any other vulnerabilities that he found in the future.

In violation of Title 18, United States Code, Section 371.

COUNT TWO
Interstate Threats
(18 U.S.C. § 875(d))

39. Paragraphs 1 through 12 and 15 through 38 are re-alleged and incorporated as if set forth herein in their entirety.

40. On or about December 1, 2007, in the District of New Hampshire and elsewhere, the defendant

ANIL KHEDA

intending to extort from a person, firm, association, and corporation, money and other things of value, transmitted in interstate and foreign commerce a communication containing a threat to injure the property and reputation of the addressee and of another. In violation of Title 18, United States Code, Section 875(d).

November 14, 2012

A TRUE BILL

/s/ Foreperson
Grand Jury Foreperson

JOHN P. KACAVAS
United States Attorney

/s/ Arnold H. Huftalen
Arnold H. Huftalen
Assistant U.S. Attorney

/s/ Mona Sedky
Mona Sedky
Trial Attorney
U.S. Department of Justice